

Amendments to the Claims:

1. (currently amended): A method of updating stored firmware of an imaging device having a first communication port connectable with a computer or network for receiving information and a second communication port for reading information from a portable memory source, the method comprising:
 - accepting a connection from the portable memory source at the second communication port;
 - accessing files stored on the portable memory source; and
 - updating the stored firmware with at least one of the files stored on the memory source.
2. (original): The method of claim 1, further comprising recognizing the portable memory source upon connection with the second communication port.
3. (original): The method of claim 1, further comprising generating an interruption signal upon connection of the portable memory source with the second communication port.
4. (original): The method of claim 1, further comprising periodically polling for connection of the portable memory source at the second communication port.
5. (original): The method of claim 1, further comprising searching the portable memory source for files.
6. (original): The method of claim 5, wherein said files are all files that can be read by the imaging device.
7. (original): The method of claim 5, wherein said files are files containing only firmware updates.

8. (original): The method of claim 5, further comprising automatically selecting a file to update firmware.
9. (original): The method of claim 5, further comprising presenting the files found in the search to a user.
10. (original): The method of claim 9, further comprising receiving at least one selection from a user, said at least one selection corresponding to at least one of the files to update firmware.
11. (original): The method of claim 8, further comprising verifying the contents of the selected file prior to updating the firmware.
12. (original): The method of claim 1, further comprising selecting at least one of the files on the portable memory device to update the firmware.
13. (original): The method of claim 1, wherein said connection between the portable memory device and the second communication port is a direct connection.
14. (original): The method of claim 1, wherein said connection between the portable memory device and the second communication port is an indirect connection.
15. (currently amended): A method of authenticating a user of an imaging device with a portable memory device connectable to ~~an~~ the imaging device, the method comprising:
communicating authentication information stored on the portable memory device to the imaging device; ~~and~~
verifying the authentication information on the portable memory device; and upon verification, granting the user access to at least one function of the imaging device.
16. (original): The method of claim, 15, wherein said authentication information is stored on the portable memory device at a location remote from the imaging device.

17. (original): The method of claim 15, further comprising printing at the imaging device a document stored from the portable memory device upon successful verification of the authentication information.

18. (original): The method of claim 15, wherein said portable memory device contains additional information other than authentication information.

19. (currently amended): The method of claim 18, further comprising executing an operation at the imaging device using at least some of the additional information stored on the portable memory device upon successful verification of the authentication information. -

20. (currently amended): The method of claim 15, further comprising updating configuration data on the imaging device from configuration information stored on the portable memory device upon successful verification of the authentication information. -

21. (original): The method of claim 20, wherein the configuration information stored on the portable memory device represents a user's configuration preferences.

22. (original): The method of claim 20, wherein the configuration of the imaging device remains updated only while the portable memory device is connected to the imaging device.

23. (currently amended): The method of claim 15, further comprising updating the firmware of the imaging device from a file stored on the portable memory device upon successful verification of the authentication information. -

24. (original): The method of claim 15, further comprising accessing personal profile information and utilizing the personal profile information to complete a base operation at the imaging device.

25. (original): The method of claim 15, further comprising accepting a connection from the portable memory device at a communication port on the imaging device.

26. (original): The method of claim 25, wherein said connection is achieved through an interface directly connected to said communication port.

27. (original): The method of claim 25, wherein said connection is achieved through an interface indirectly connected to said communication port.

28. (original): The method of claim 15, wherein the authentication information is time sensitive.

29. (original): The method of claim 28, further comprising updating said time sensitive authentication information when said portable memory device is connected to said imaging device.

30. (currently amended): A method of printing a document from a location remote from a printer, the method comprising:

receiving at said printer information which is from the location and which is to be printed;

accepting a connection from a portable memory device at the printer;

verifying authentication information stored on the portable memory device; and
upon verification, printing at the printer the received information.

31. (original): The method of claim 30, wherein said connection from the portable memory device is a direct connection.

32. (original): The method of claim 30, wherein said connection from the portable memory device is an indirect connection.

Serial No.: 10/781,529
Attorney Docket No.: 2003-0689.01
Amendment

33. (original): The method of claim 30, wherein verifying authentication information further comprises comparing said authentication information with information stored on a network server.